Investigation detects cyber espionage network

April 1 2009

(PhysOrg.com) -- The Information Warfare Monitor - a joint effort of the SecDev Group (Ottawa) and the Citizen Lab (University of Toronto) - detected a cyber espionage network involving over 1,295 compromised computers in 103 countries.

As explained during a U of T news conference, Close to 30 per cent of the compromised computers are considered high value targets. They include the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN Secretariat, SAARC, and the Asian Development Bank, news organizations, and an unclassified computer located at NATO headquarters.

The report, entitled Tracking GhostNet: Investigating a Cyber Espionage Network, is a
product of a two-phase 10-month investigation, consisting of fieldwork, technical scouting, and laboratory analysis. The research began by focusing on allegations of Chinese cyber espionage against the Tibetan community in exile, and eventually led to a much wider network of compromised machines.

Investigators conducted field research in India, Europe and North America, including in the private office of the Dalai Lama, the Tibetan Government-in-Exile, and several Tibetan NGOs.

According to IWM investigator Greg Walton, "We uncovered real-time

evidence of malware that had penetrated Tibetan computer systems, extracting sensitive documents from the private office of the Dalai Lama."

During the second phase of the investigation, the data led to the discovery of insecure, web-based interfaces to four control servers. The interfaces allow attacker(s) to send instructions to and receive data from compromised computers.

"What we found is not so much unprecedented in scope and sophistication," said Nart Villeneuve, a senior IWM analyst ,"but the relatively small size of the network and concentration of high value targets is significant. It does not fit the profile for a typical cyber crime network."

According to IWM principal investigators Ron Deibert of Citizen Lab, a professor at U of T's Munk Centre for International Studies, and Rafal Rohozinski (SecDev Group), "This report serves as a wake-up call. At the very least, the large percentage of high-value targets compromised by this network demonstrates the relative ease with which a technically unsophisticated approach can quickly be harnessed to create a very effective spynet...These are major disruptive capabilities that the professional information security community, as well as policymakers, need to come to terms with rapidly."

Provided by University of Toronto (news : web)